AMENDMENTS TO THE CLAIMS

1-13. (Canceled)

14. (Currently Amended) A license ~~information~~ ticket management apparatus which manages a license ~~information~~ ticket that includes (i) an encrypted content key for decrypting encrypted digital content and (ii) content reproduction condition information indicating a range in which the digital content can be used, said apparatus comprising:

a storage unit not having tamper resistance; and

a tamper resistance module which encrypts at least the license ~~information~~ticket, among the license ~~information~~ ticket and a correspondence table for managing an update history of the license ~~information~~ticket, and which stores the encrypted license ~~information~~ ticket into the storage unit,

wherein the tamper resistance module includes:

a digital signature management unit configured to (i) generate a hash value of the encrypted license ~~information~~ ticket before the encrypted license ticket ~~information~~ is stored into the storage unit, and store the generated hash value into a built-in memory, and (ii) read the encrypted license ticket ~~information~~ stored in the storage unit, generate a hash value of the read encrypted license ticket~~information~~, and compare the hash value stored in the built-in memory with the generated hash value of the read encrypted license ticket~~information~~, with a result of the comparison being used to verify validity of the read encrypted license ticket~~information~~, the validity indicating that the read encrypted license ticket ~~information~~ has not been tampered with;

an encrypting and decrypting unit configured to (i) encrypt the license ticket ~~information~~ and store the encrypted license ticket ~~information~~ in the storage unit, and (ii) read the encrypted license ticket ~~information~~ from the storage unit and decrypt the read encrypted license ticket~~information~~; and

a control unit configured to decrypt the encrypted content key included in the license ticket ~~information~~ decrypted by the encrypting and decrypting unit, output the decrypted content key outside of the license ticket ~~information~~ management apparatus, update the content reproduction condition information included in the decrypted license ticket~~information~~, and cause the encrypting and decrypting unit to encrypt the updated license ticket ~~information~~ and to overwrite the encrypted license ticket ~~information~~ stored in the storage unit with the encrypted updated license ticket ~~information~~ so as to store the encrypted updated license ticket ~~information~~ into the storage unit, when the digital content is used and only when the digital signature management unit verifies the validity of the read encrypted license ticket~~information~~, and

wherein the decrypted content key outputted by the control unit is received and used for decrypting the digital content by a content decrypting unit that is connected to the license ticket ~~information~~ management apparatus.

15. (Currently Amended) The license ticket ~~information~~ management apparatus according to Claim 14,

wherein the license ticket ~~information~~ further includes a digital signature for (i) the encrypted content key and (ii) the content reproduction condition information,

wherein the encrypting and decrypting unit is configured to encrypt each of a plurality of ~~pieces of license information~~license tickets, and store each ~~piece of~~ encrypted license ticket ~~information~~ in the storage unit, and wherein the digital signature management unit is configured to, for ~~a set of all~~each of the ~~pieces of~~ encrypted license tickets~~information~~, (i) generate a hash value of the digital signature included in the encrypted license ticket ~~information~~ before the encrypted license ticket ~~information~~ is stored into the storage unit, and store the generated hash value into the built-in memory, and (ii) read the encrypted license ticket ~~information~~ stored in the storage unit, generate a hash value of the digital signature included in the read encrypted license ticket~~information~~, and compare the hash value stored in the built-in memory with the generated hash value of the digital signature included in the read encrypted license ticket~~information~~, with a result of the comparison being used to verify validity of the read encrypted license ticket~~information~~, the validity indicating that the read encrypted license ticket ~~information~~ has not been tampered with.

16. (Currently Amended) The license ticket ~~information~~ management apparatus according to Claim 14,

wherein the encrypting and decrypting unit is further configured to (i) encrypt the correspondence table and store the encrypted correspondence table in the storage unit, and (ii) read the stored correspondence table from the storage unit and decrypt the read correspondence table, the correspondence table being a table in which identification information identifying the license ticket ~~information~~ is stored in association with information indicating an update history of the license ticket ~~information~~ for each of a plurality of ~~pieces of~~ license ~~information~~ tickets stored in the storage unit, and

wherein the digital signature management unit is configured to (i) generate a hash value of the encrypted correspondence table before the encrypted correspondence table is stored into the storage unit, and store the generated hash value into the built-in memory, and (ii) read the encrypted correspondence table stored in the storage unit, generate a hash value of the read encrypted correspondence table, and compare the hash value stored in the built-in memory with the generated hash value of the read encrypted correspondence table, with a result of the comparison being used to verify validity of the read encrypted correspondence table, the validity indicating that the read encrypted correspondence table has not been tampered with.

17. (Currently Amended) The license ticket ~~information~~ management apparatus according to Claim 16,

wherein corresponding information indicating the update history indicates the number of updates or a random number, the corresponding information being included in the correspondence table decrypted by the encrypting and decrypting unit, and

wherein the control unit is further configured to update the corresponding information of the correspondence table indicating the number of updates or the random number, when the license ticket ~~information~~ is updated, and cause the encrypting and decrypting unit to encrypt the updated correspondence table and to overwrite the encrypted correspondence table stored in the storage unit with the encrypted updated correspondence table so as to store the encrypted updated correspondence table into the storage unit.

18. (Currently Amended) The license ticket ~~information~~ management apparatus according to Claim 14,

wherein the control unit is further configured to determine whether or not the license ticket ~~information~~ is new, and cause the encrypting and decrypting unit to encrypt the license ticket~~information~~, which is determined to be new, and to overwrite the encrypted license ticket

~~information~~ stored in the storage unit with the new encrypted license ticket ~~information~~ so as to store the new encrypted license ticket ~~information~~ into the storage unit.

19. (Currently Amended) The license ticket ~~information~~ management apparatus according to Claim 14,

wherein the tamper resistance module includes an IC card, and

wherein the storage unit includes a flash memory.

20. (Currently Amended) A license ticket ~~information~~ management method for managing, by using a tamper resistance module, a license ticket ~~information~~ that includes (i) an encrypted content key for decrypting encrypted digital content and (ii) content reproduction condition information indicating a range in which the digital content can be used, the tamper resistance module comprising a digital signature management unit, an encrypting and decrypting unit, and a control unit, and the tamper resistance module being capable of writing and reading encrypted information to a storage unit having no tamper resistance, encrypting at least the license ticket~~information~~, among the license ticket ~~information~~ and a correspondence table for managing an update history of the license ticket~~information~~, and storing the encrypted license ticket ~~information~~ into the storage unit, said method comprising:

a digital signature management step, being performed by the digital signature management unit, of (i) generating a hash value of the encrypted license ticket ~~information~~ before the encrypted license ticket ~~information~~ is stored into the storage unit, and storing the generated hash value into a built-in memory, and (ii) reading the encrypted license ticket ~~information~~ stored in the storage unit, generating a hash value of the read encrypted license ticket~~information~~, and comparing the hash value stored in the built-in memory with the generated hash value of the read encrypted license ticket~~information~~, with a result of the comparison being used to verify validity of the read encrypted license ticket~~information~~, the validity indicating that the read encrypted license ticket ~~information~~ has not been tampered with;

an encrypting and decrypting step, being performed by the encrypting and decrypting unit, of (i) encrypting the license ticket ~~information~~ and storing the encrypted license ticket ~~information~~ in the storage unit, and (ii) reading the encrypted license ticket ~~information~~ from the storage unit and decrypting the read encrypted license ticket~~information~~; and

a control step, being performed by the control unit, of decrypting the encrypted content key included in the license ticket ~~information~~ decrypted in the encrypting and decrypting step, outputting the decrypted content key outside a license ticket ~~information~~ management apparatus, updating the content reproduction condition information included in the decrypted license ticket~~information~~, and causing the updated license ticket ~~information~~ to be encrypted in the encrypting and decrypting step and the encrypted license ticket ~~information~~ stored in the storage unit to be overwritten with the encrypted updated license ticket ~~information~~ so as to store the encrypted updated license ticket ~~information~~ into the storage unit,

wherein the decrypted content key outputted in said control step is received and used for decrypting the digital content by a content decrypting unit that is connected to the license ticket ~~information~~ management apparatus.

21. (Currently Amended) A non-transitory computer-readable medium encoded with a program having computer-executable instructions, the program being for use in a license ticket ~~information~~ management apparatus which manages, by using a tamper resistance module, a license ticket ~~information~~ that includes (i) an encrypted content key for decrypting encrypted digital content and (ii) content reproduction condition information indicating a range in which the digital content can be used, the tamper resistance module comprising a digital signature management unit, an encrypting and decrypting unit, and a control unit, and the tamper resistance module being capable of writing and reading encrypted information to a storage unit storing the encrypted information and having no tamper resistance, encrypting at least the license ticket~~information~~, among the license ticket ~~information~~ and a correspondence table for managing an update history of the license ticket~~information~~, and storing the encrypted license ticket ~~information~~ into the storage unit, wherein execution of the computer-executable instructions by a computer causes the computer to execute a method comprising:

a digital signature management step, being performed by the digital signature management unit, of (i) generating a hash value of the encrypted license ticket ~~information~~ before the encrypted license ticket ~~information~~ is stored into the storage unit, and storing the generated hash value into a built-in memory, and (ii) reading the encrypted license ticket ~~information~~ stored in the storage unit, generating a hash value of the read encrypted license ticket~~information~~, and comparing the hash value stored in the built-in memory with the generated hash value of the read encrypted license ticket~~information~~, with a result of the comparison being used to verify validity of the read encrypted license ticket~~information~~, the validity indicating that the read encrypted license ticket ~~information~~ has not been tampered with;

an encrypting and decrypting step, being performed by the encrypting and decrypting unit, of (i) encrypting the license ticket ~~information~~ and storing the encrypted license ticket ~~information~~ in the storage unit, and (ii) reading the encrypted license ticket ~~information~~ from the storage unit and decrypting the read encrypted license ticket~~information~~; and a control step, being performed by the control unit, of decrypting the encrypted content key included in the license ticket ~~information~~ decrypted in the encrypting and decrypting step, outputting the decrypted content key outside a license ticket ~~information~~ management apparatus, updating the content reproduction condition information included in the decrypted license ticket~~information~~, and causing the updated license ticket ~~information~~ to be encrypted in the encrypting and decrypting step and the encrypted license ticket ~~information~~ stored in the storage unit to be overwritten with the encrypted updated license ticket ~~information~~ so as to store the encrypted updated license ticket ~~information~~ into the storage unit,

wherein the decrypted content key outputted in said control step is received and used for decrypting the digital content by a content decrypting unit that is connected to the license ticket ~~information~~ management apparatus.

22. (New) A license ticket management apparatus which manages a license ticket that includes (i) an encrypted content key for decrypting encrypted digital content and (ii) content reproduction condition information indicating a range in which the digital content can be used, said apparatus comprising:

a storage unit not having tamper resistance; and

a tamper resistance module which encrypts at least the license ticket, among the license ticket and a correspondence table for managing an update history of the license ticket, and which stores the encrypted license ticket into the storage unit,

wherein the tamper resistance module includes:

a digital signature management means for (i) generating a hash value of the encrypted license ticket before the encrypted license ticket is stored into the storage unit, and storing the generated hash value into a built-in memory, and (ii) reading the encrypted license ticket stored in the storage unit, generating a hash value of the read encrypted license ticket, and comparing the hash value stored in the built-in memory with the generated hash value of the read encrypted license ticket, with a result of the comparison being used to verify validity of the read encrypted license ticket, the validity indicating that the read encrypted license ticket has not been tampered with;

an encrypting and decrypting means for (i) encrypting the license ticket and storing the encrypted license ticket in the storage unit, and (ii) reading the encrypted license ticket from the storage unit and decrypting the read encrypted license ticket; and

a control means for decrypting the encrypted content key included in the license ticket decrypted by the encrypting and decrypting means, outputting the decrypted content key outside of the license ticket management apparatus, updating the content reproduction condition information included in the decrypted license ticket, and causing the encrypting and decrypting means to encrypt the updated license ticket and to overwrite the encrypted license ticket stored in the storage unit with the encrypted updated license ticket so as to store the encrypted updated license ticket into the storage unit, when the digital content is used and only when the digital signature management means verifies the validity of the read encrypted license ticket, and

wherein the decrypted content key outputted by the control means is received and used for decrypting the digital content by a content decrypting unit that is connected to the license ticket management apparatus.

23. (New) The license ticket management apparatus according to Claim 22, wherein the license ticket further includes a digital signature for (i) the encrypted content key and (ii) the content reproduction condition information,

wherein the encrypting and decrypting means encrypts each of a plurality of license tickets, and stores each encrypted license ticket in the storage unit, and

wherein, for each of the encrypted license tickets, the digital signature management means (i) generates a hash value of the digital signature included in the encrypted license ticket before the encrypted license ticket is stored into the storage unit, and stores the generated hash value into the built-in memory, and (ii) reads the encrypted license ticket stored in the storage unit, generates a hash value of the digital signature included in the read encrypted license ticket, and compares the hash value stored in the built-in memory with the generated hash value of the digital signature included in the read encrypted license ticket, with a result of the comparison being used to verify validity of the read encrypted license ticket, the validity indicating that the read encrypted license ticket has not been tampered with.

24. (New) The license ticket management apparatus according to Claim 22,

wherein the encrypting and decrypting means (i) encrypts the correspondence table and stores the encrypted correspondence table in the storage unit, and (ii) reads the stored correspondence table from the storage unit and decrypts the read correspondence table, the correspondence table being a table in which identification information identifying the license ticket is stored in association with information indicating an update history of the license ticket for each of a plurality of license tickets stored in the storage unit, and

wherein the digital signature management means (i) generates a hash value of the encrypted correspondence table before the encrypted correspondence table is stored into the storage unit, and stores the generated hash value into the built-in memory, and (ii) reads the encrypted correspondence table stored in the storage unit, generates a hash value of the read encrypted correspondence table, and compares the hash value stored in the built-in memory with the generated hash value of the read encrypted correspondence table, with a result of the comparison being used to verify validity of the read encrypted correspondence table, the validity indicating that the read encrypted correspondence table has not been tampered with.

25. (New) The license ticket management apparatus according to Claim 24,

wherein corresponding information indicating the update history indicates the number of updates or a random number, the corresponding information being included in the correspondence table decrypted by the encrypting and decrypting means, and

wherein the control means updates the corresponding information of the correspondence table indicating the number of updates or the random number, when the license ticket is updated, and causes the encrypting and decrypting means to encrypt the updated correspondence table and to overwrite the encrypted correspondence table stored in the storage unit with the encrypted updated correspondence table so as to store the encrypted updated correspondence table into the storage unit.

26. (New) The license ticket management apparatus according to Claim 22,

wherein the control means determines whether or not the license ticket is new, and causes the encrypting and decrypting means to encrypt the license ticket, which is determined to be new, and to overwrite the encrypted license ticket stored in the storage unit with the new encrypted license ticket so as to store the new encrypted license ticket into the storage unit.

27. (New) The license ticket management apparatus according to Claim 22,

wherein the tamper resistance module includes an IC card, and

wherein the storage unit includes a flash memory.